IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for dynamically managing security associated with document collaboration, comprising:

associating collaborators with different encrypted versions of a key, wherein decrypted versions of the key permit access to a document; and

adding an identity service as one of the collaborators, wherein the identity service is capable of dynamically adjusting encryption formats for one or more of the collaborators' encrypted keys, and wherein a trust specification is associated with the document and a particular collaborator, the trust specification identifies a contract that defines a relationship between the particular collaborator and the document, and wherein the contract defines policies, authentication requirements, and identity information required before the particular collaborator is dynamically added to or removed from the collaborators that have access to the document.

2. (Original) The method of claim 1 further comprising, dynamically adding or removing one or more of the collaborators.

3. (Original) The method of claim 1 further comprising, linking the collaborators and encrypted keys to the document as metadata defining document access and security.

4. (Original) The method of claim 1 further comprising, embedding the collaborators and encrypted keys within a portion of the document defining document access and security.

5. (Original) The method of claim 1 wherein adding further includes recognizing a select one of the collaborators as trusted to the identity service and permitting it to provide a dynamically generated public key which the identity service uses to encrypt a select one of the encrypted keys associated with the trusted collaborator.

6. (Original) The method of claim 5 wherein adding further includes inspecting a community list associated with the document to determine if the select one of the collaborators is authorized to be the trusted.

7. (Original) The method of claim 1 signing the document by a select one of the collaborators which modifies the document, wherein the signature is associated with a public key of the select collaborator.

8. (Original) The method of claim 1 further comprising:

changing the key; and

updating the encrypted versions of the key with the changed key.

9. (Currently Amended) A method for dynamically managing security associated with document collaboration, comprising:

identifying a collaborator associated with a document;

verifying a trust relationship between the collaborator and the document;

acquiring a dynamic public key from or on behalf of the collaborator;

decrypting a symmetric key which grants access to the document; and

encrypting the symmetric key with the dynamic public key, and wherein a trust specification is associated with the document and the collaborator, the trust specification identifies a contract that defines the trust relationship between the collaborator and the document, and wherein the contract defines policies, authentication requirements, and identity information required before the collaborator is verified for access to the document.

10. (Original) The method of claim 9 further comprising:

recognizing that the collaborator has altered the document and signed the document with the dynamic public key; and

communicating the dynamic public key to a plurality of other collaborators associated with the document.

11. (Original) The method of claim 9 wherein acquiring further includes acting as an intermediary between the collaborator and key service for purposes of acquiring a strongly rooted key pair for the collaborator, wherein a portion of that key pair is the public key and wherein another portion of that key pair is a private key which permits the collaborator to decrypt the encrypted symmetric key for purposes of accessing the document.

12. (Original) The method of claim 9 wherein acquiring further includes generating a non-strongly rooted private-public key pair for the collaborator.

13. (Currently Amended) The method of claim 9 further comprising:

dynamically receiving a request from a different collaborator to access the document;

inspecting the [[a]] trust specification to ensure the access is permissible;

receiving a public key for the different collaborator;

generating a new symmetric key which includes the different collaborator, the collaborator, and other collaborators associated with the document; and

encrypting the symmetric key with the public key of the different collaborator and with the dynamic public key of the collaborator and with other public keys associated with the other collaborators.

14. (Original) The method of claim 13 further comprising, communicating the public key of the different collaborator to the collaborator and to the other collaborators associated with the document.

15. (Original) The method of claim 13 wherein generating further includes generating a random new symmetric key.

16. (Original) The method of claim 13 wherein inspecting further includes inspecting community lists associated with the different collaborator and the document to ensure that the different collaborator can be dynamically added as a new collaborator to the document.

17. (Original) The method of claim 9 wherein verifying further includes authenticating the collaborator to the document according to a contract.

18. (Currently Amended) A dynamic collaborative document security system, comprising:

a document;

a list of collaborators associated with the document; and

an identity service, wherein the identity service is included within the list of collaborators, and wherein the identity service dynamically manages encryption of a symmetric key associated with the document and dynamically manages identities of the list of collaborators according to a trust specification, wherein access to a decrypted version of the symmetric key provides access to the document, and wherein the document maintains the list of collaborators and the list of collaborators includes identities for each unique collaborator that can permissibly access the document.

19. (Original) The dynamic collaborative document security system of claim 18 wherein each entry within the list of collaborators includes a specific encrypted version of the symmetric key, each specific encrypted version is encrypted with a specific public key of a specific collaborator included within the list of collaborators.

20. (Original) The dynamic collaborative document security system of claim 18 wherein the identity service changes the symmetric key and re-performs encryption when a specific collaborator is dynamically added to or dynamically removed from the list of collaborators.

21. (Original) The dynamic collaborative document security system of claim 18 wherein the identity service dynamically acquires a strongly rooted public-private key pair on behalf of a requesting collaborator from a keying service.

22. (Original) The dynamic collaborative document security system of claim 18 wherein the identity service dynamically generates a non-strongly rooted public-private key pair on behalf of

a requesting collaborator.

23. (Original) The dynamic collaborative document security system of claim 18 wherein the identity service determines if a dynamically generated public key associated with a specific collaborator of the list of collaborators has signed the document after altering the document, and wherein if this occurs the identity service communicates the dynamically generated public key to the remaining collaborators included within the list of collaborators.

24. (Original) The dynamic collaborative document security system of claim 18 further comprising access control rights associated with each collaborator included within the list of collaborators.

25. (Currently Amended) A document residing in a computer readable medium, comprising:

a document having content data, the symmetric key and a list of collaborators;

the [[a]] symmetric key; and

the [[a]] list of collaborators, each collaborator within the list associated with a specific encrypted version of the symmetric key, wherein an identity service is included within the list of collaborators, the identity service capable of dynamically adding and removing select ones of the collaborators and capable of dynamically re-encrypting the symmetric key for the select ones of the collaborators, and wherein the document maintains the list of collaborators and the list of collaborators includes identities for each unique collaborator that can permissibly access the document.

26. (Cancelled).

27. (Original) The document of claim 25, wherein the symmetric key and the list of collaborators are metadata linked with the content data.

28. (Original) The document of claim 25 further comprising, a trust specification that defines relationships between collaborators and the document, and wherein the trust specification drives

the actions of the identity service.

29. (Original) The document of claim 25 further comprising, a community list which is consumed by the identity service, the community list identifying collaborators which can be dynamically added to the list of collaborators.

30. (Original) The document of claim 25 wherein members of the list of collaborators have been granted access control rights or edit rights to the document via the identity service which determines the access control rights or edit rights based on a trust specification for the document.

31. (Original) The document of claim 25 wherein the identity service communicates a trust specification of the document dynamically to another service, and wherein that service uses the trust specification to dynamically manage access to the document.